UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/575,749	05/22/2000	William P. Alberth Jr.	CS10614	1184

7590 06/16/2006

Motorola Inc
Intellectual Property Dept(BMM)
600 North US Highway 45 AN475
Libertyville, IL 60048

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 06/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/575,749	ALBERTH JR. ET AL.	
	Examiner	Art Unit	
	Kyung H. Shin	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 3/14/2006, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

2. Claims **1 - 19** are pending. Claims **1, 8, 14, 15** are amended. Claims **18, 19** are new. Independent claims are **1, 8, 14, 18**.

Claim Rejection - 35 USC § 103

The text of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3. **Claims 1 - 17** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Storck et al.** (US Patent No. 5,434,395) in view of **Kawan et al.** (US Patent No. 6,289,324) and further in view of **Kramer et al.** (US Patent No. 6,324,525) and further in view of **Findley, Jr et al.** (US Patent No. 5,979,773).

Regarding Claim 1, Storck discloses a personal data storage apparatus comprised of:

c) a second interface circuit coupled to said memory device and providing communications access to the second personal data storage device. (see Storck col. 11, lines 34-51; col. 5, lines 16-24: interface circuit for data transfer between two data carriers or smart cards (i.e. data storage devices))

a) a first user personal data storage device including a memory device storing; (see Storck col. 11, lines 52-56: smart card memory utilization)

i) a first set of user data; (see Storck col. 11, lines 43-51: data storage)

ii) Storck discloses the usage of encryption technology. (see Storck col. 2, lines 58-59; col. 19, lines 56-59: encryption security techniques) Storck does not specifically disclose the usage of encryption keys for secure protection of data. However, Kawan discloses the usage of encryption keys with a first encryption key for encrypting at least part of said first set of user data; (see Kawan col. 5, lines 52-56; col. 9, lines 2-26; col. 10, lines 7-17: encryption keys used for secure protection of data)

b) Storck discloses the usage of smart card technology for transactions implementing split authorization which allows access only when two data carriers or smart cards are coupled together. (i.e. only when a second personal data storage device is operatively coupled to said first personal data storage device) (see Storck col. 12, lines 45-48; col. 5, line 64; col. 6, line 9) Storck does not specifically disclose a three party transaction between multiple devices. However, Kramer discloses a three party transaction, a first interface circuit coupled to said memory device granting conditional access to a third device to data therein using an appropriate data exchange protocol between the first personal data storage device and the third device; (see Kramer col. 4, lines 57-65; col. 140, lines 39-42: three party transactions utilizing smart card technology), and Findley discloses wherein smart card technology for transactions implementing split authorization which allows access only when two data carriers or smart cards are coupled together (see Findley col. 3, lines 46-51; col. 6, lines 31-33; col. 7, lines 59-65: dual card access system, both cards must be coupled together to be accessible; col. 2, lines 30-36: three card transaction capability).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Storck to securely protect data utilizing encryption keys as taught by Kawan, and to enable performing a three party transaction utilizing smart card type devices as taught by Kramer, and to utilize smart card access and processing technologies requiring dual smart cards that are operatively coupled as taught by Findley. One of ordinary skill in the art would be motivated to employ Kawan in order to

offer enhanced convenience and security completing transactions utilizing smart card technology (see Kawan col. 2, lines 12-17: " *... smart card that offers enhanced convenience when assisting a customer in executing a transaction ... smart card that can acquire information regarding a consumer's transactions and establish a system automated task for carrying out such financial transactions ...* "), and to employ Kramer in order to enable optimum and secure two party and three party electronic transactions (see Kramer col. 3, lines 42-46: " *... allows for robustly secure two-party data transmission ... meet the ultimate need of the electronic commerce market for robustly secure three-party data transmission ...* "), and to employ Findley in order to enable enhanced and automated user access security features within a network environment (see Findley col. 2, lines 30-32: " *... automatic system and methods for identifying people or personnel and providing secured access to a facility of authorized personnel upon verifying the identity of such personnel ... means of, and methods for, providing automatic, rapid and positive verification of persons who previously have been authorized access to secured areas. ...* ").

Regarding Claims 2, 9, Storck discloses the personal data storage apparatus of claim 1 further comprised of a processor (see Storck col. 1, lines 33-36), operatively coupled to said memory device and to said first and second interface circuits (see Storck col. 12, lines 7-18; col. 5, lines 42-47: coupled data carriers in communications for transactions), and Findley discloses wherein a first and second card operatively coupled. (see Findley col. 3, lines 46-51; col. 6, lines 31-33; col. 7, lines 59-65: dual card access system, both cards must be coupled together to be accessible).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Storck to utilize smart card access and processing technologies requiring dual smart cards that are operatively coupled as taught by Findley. One of ordinary skill in the art would be motivated to employ Findley in order to enable enhanced and automated user access security features within a network environment. (see Findley col. 2, lines 30-32)

Regarding Claims 3, 10, Storck discloses the personal data storage apparatus of claim 1 wherein said second personal data storage device is operatively coupled to said first personal storage device using a mechanical coupling. (see Storck col. 18, lines 31-38; col. 5, lines 51-63: connection for data carrier (i.e. smart card) transactions)

Regarding Claim 4, Storck discloses the personal data storage apparatus of claim 3 wherein said mechanical coupling is a connector. (see Storck col. 10, line 11-13: connector utilized for communications between data carriers)

Regarding Claims 5, 11, Storck discloses the personal data storage apparatus of claim 1 wherein said second personal data storage device is operatively coupled to said first personal storage device using a wireless connection (see Storck col. 19, lines 14-22: infrared (i.e. wireless) communications), and Findley discloses wherein a second personal data storage device operatively coupled to said first personal storage device (see Findley col. 3, lines 46-51; col. 6, lines 31-33; col. 7, lines 59-65: dual card access

system, both cards must be coupled together to be accessible).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Storck to utilize smart card access and processing technologies requiring dual smart cards that are operatively coupled as taught by Findley. One of ordinary skill in the art would be motivated to employ Findley in order to enable enhanced and automated user access security features within a network environment. (see Findley col. 2, lines 30-32)

Regarding Claims 6, 12, Storck discloses the personal data storage apparatus of claim 5 wherein said wireless connection is a radio link. (see Storck Fig. 15; col. 8, line 18-21: radio frequency (i.e. wireless) communications)

Regarding Claims 7, 13, 16, Storck discloses the personal data storage apparatus of claim 1, where an agent of the issuer of the personal data storage apparatus can recreate the user data from a single part of the personal data storage apparatus. (see Storck col. 7, lines 5-16; col. 11, lines 52-56; col. 12, lines 15-18: data copy techniques, transfer of data between different memory regions of data carrier (i.e. smart card))

Regarding Claim 8, Storck discloses a personal data storage apparatus comprised of:

b) a second personal data storage device coupled to said first personal data storage device and being comprised of:

i) a second memory device storing; (see Storck col. 11, lines 52-56: smart card memory)

1) a substantially duplicate copy of said first set of user data; (see Storck col. 12, lines 24-26: data copied from one data carrier or smart card to another (i.e. all data on card equals duplicate copy))

d) whereby user data in either said first or second personal data storage device is accessible and usable only when said first and second personal data storage devices are in communication with each other (see Storck col. 12, lines 45-48: split authorization requires both data carriers (i.e. smart cards) coupled together, data transactions only possible when two data carriers are coupled together), and Findley discloses wherein user data in either said first or second personal data storage device is accessible and usable only when said first and second personal data storage devices are in communication with each other (see Findley col. 3, lines 46-51; col. 6, lines 31-33; col. 7, lines 59-65: dual card access system, both cards must be coupled together to be accessible).

a) a first personal data storage device comprising:

i) a first memory device storing; (see Storck col. 11, lines 52-56: smart card memory)

1) a first set of user data; (see Storck col. 11, lines 43-51: smart card user data stored)

2) Storck discloses the usage of encryption technology. (see Storck col. 2, lines 58; col. 19, lines 56-59: encryption security techniques) Storck does

not specifically disclose the usage of encryption keys in the secure protection of data. However, Kawan discloses the usage of encryption keys with a first encryption key for encrypting at least part said first set of user data; (see Kawan col. 5, lines 52-56; col. 9, lines 2-26; col. 10, lines 7-17: encryption key utilization for secure protection of data carrier (i.e. smart card) data)

ii) a first interface circuit coupled to said memory device granting conditional access to data therein using a predetermined protocol and only when a second personal data storage device is operatively coupled to said first personal data storage device; (see Storck col. 11, lines 18; col. 12, lines 45-48: data transaction between two data carriers (i.e. smart cards)), and Findley discloses wherein only when a second personal data storage device is operatively coupled to said first personal data storage device (see Findley col. 3, lines 46-51; col. 6, lines 31-33; col. 7, lines 59-65: dual card access system, both cards must be coupled together to be accessible).

iii) a second interface circuit coupled to said memory device and providing access to a second personal data storage device; (see Storck col. 11, lines 34-51; col. 5, lines 16-24: interface circuit for transactions between two data carriers (i.e. smart cards))

c) Storck discloses the usage of encryption technology. (see Storck col. 2, lines 58; col. 19, lines 56-59) Storck does not specifically disclose the usage of encryption keys in the secure protection of data. However, Kawan discloses the usage of

encryption keys with a second encryption key for encrypting at least part said first set of user data; (see Kawan col. 5, lines 52-56; col. 9, lines 2-26; col. 10, lines 7-17: encryption key utilization for secure protection of data carrier (i.e. smart card) data)

ii) Storck discloses a second interface circuit coupled to said memory device granting conditional access to data therein using a predetermined protocol and only when said second personal data storage device is operatively coupled to said first personal data storage device; (see Storck col. 12, lines 45-48: split authorization requires two data carriers (i.e. smart cards) coupled before data transactions) Storck does not disclose three party transactions. However, Kramer discloses granting access to data when said second personal data storage device is operatively coupled to said first personal data storage device (i.e. a three party transaction)) (see Kramer col. 4, lines 57-65; col. 140, lines 39-42: three party transactions utilizing smart card technology), and Findley discloses wherein granting access to data when said second personal data storage device is operatively coupled to said first personal data storage device (see Findley col. 3, lines 46-51; col. 6, lines 31-33; col. 7, lines 59-65: dual card access system, both cards must be coupled together to be accessible).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Storck to securely protect data utilizing encryption keys as taught by Kawan and to enable performing a three party transaction utilizing smart

card type devices as taught by Kramer, and to utilize smart card access and processing technologies requiring dual smart cards that are operatively coupled as taught by Findley. One of ordinary skill in the art would be motivated to employ Kawan in order to offer enhanced convenience and security completing transactions utilizing smart card technology (see Kawan col. 2, lines 12-17), and to employ Kramer in order to enable optimum and secure two party and three party electronic transactions (see Kramer col. 3, lines 42-46), and to employ Findley in order to enable enhanced and automated user access security features within a network environment (see Findley col. 2, lines 30-32).

Regarding Claim 14, Storck discloses a method of securing access to data stored in a personal data storage device comprised of the steps of:

a) storing personal data in first and second data storage devices that are capable of being operable coupled to each other; (see Storck col. 5, lines 1-7: data carriers (i.e. smart cards) coupled together for data transactions)

b) Storck discloses the usage of encryption technology. (see Storck col. 2, lines 58; col. 19, lines 56-59: encryption security techniques) Storck does not specifically disclose the usage of encryption keys in the secure protection of data. However, Kawan discloses the usage of encryption keys for encrypting said personal data in a first data storage device using a first encryption key and encrypting it in said second device using a second encryption key; (see Kawan col. 5, lines 52-56; col. 9, lines 2-26; col. 10, lines 7-17: encryption keys for secure protection of data carrier (i.e. smart card) data)

c) Storck discloses the usage of smart card technology for transactions. (see Storck col. 12, lines 45-48; col. 5, line 64; col. 6, line 9) Storck does not specifically disclose a three party transaction between multiple devices. However, Kramer discloses a three party transaction, granting access to a third device to said personal data in either said first data storage device or said second data storage device only when said first and second storage devices are operatively coupled together (see Kramer col. 4, lines 57-65; col. 140, lines 39-42: three party transactions utilizing smart card technology), and Findley discloses wherein a three party transaction, granting access to a third device to said personal data in either said first data storage device or said second data storage device only when said first and second storage devices are operatively coupled together (see Findley col. 3, lines 46-51; col. 6, lines 31-33; col. 7, lines 59-65: dual card access system, both cards must be coupled together to be accessible; col. 2, lines 30-36: three card transaction capability).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Storck to securely protect data utilizing encryption keys as taught by Kawan and to enable performing a three party transaction utilizing three smart card type devices as taught by Kramer, and to utilize smart card access and processing technologies requiring dual smart cards that are operatively coupled as taught by Findley. One of ordinary skill in the art would be motivated to employ Kawan in order to offer enhanced convenience and security completing transactions utilizing smart card technology (see Kawan col. 2, lines 12-17) and to employ Kramer in order to

enable optimum and secure two party and three party electronic transactions (see Kramer col. 3, lines 42-46), and to employ Findley in order to enable enhanced and automated user access security features within a network environment (see Findley col. 2, lines 30-32).

Regarding Claim 15, Storck discloses said first and second personal data storage devices are operatively coupled together through at least one of either a wireless data link or a mechanical connector. (see Storck col. 5, lines 1-7; col. 12, lines 45-48; col. 4, lines 31-34: split data carrier (i.e. smart card) authorization equals operatively coupled together data carriers (i.e. smart cards)) Storck does not specifically disclose the utilization of three party (i.e. three devices) transactions. However, Kramer discloses the method of claim 14 wherein said step of granting access to a third device to said personal data in either said first data storage device or said second data storage device only when said first and second personal data storage devices are operatively coupled together (see Kramer col. 4, lines 57-65; col. 140, lines 39-42: three party transaction utilizing smart card technology), and Findley discloses wherein said step of granting access to a third device to said personal data in either said first data storage device or said second data storage device only when said first and second personal data storage devices are operatively coupled together (see Findley col. 3, lines 46-51; col. 6, lines 31-33; col. 7, lines 59-65: dual card access system, both cards must be coupled together to be accessible; col. 2, lines 30-36: three card transaction capability).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Storck to enable performing three party transactions

utilizing smart card type devices as taught by Kramer, and to utilize smart card access and processing technologies requiring dual smart cards that are operatively coupled as taught by Findley. One of ordinary skill in the art would be motivated to employ Kramer in order to enable optimum and secure two party and three party electronic transactions (see Kramer col. 3, lines 42-46), and to employ Findley in order to enable enhanced and automated user access security features within a network environment (see Findley col. 2, lines 30-32).

Regarding Claim 17, Storck discloses the usage of encryption technology. (see Storck col. 2, lines 58; col. 19, lines 56-59: encryption security techniques) Storck does not specifically disclose the usage of encryption keys in the secure protection of data. However, Kawan discloses the method of claim 14 wherein said first and second encryption keys are same. (see Kawan col. 5, lines 52-56; col. 9, lines 2-26; col. 10, lines 7-17; col. 4, lines 66-67: encryption keys utilization for protection of data, symmetric keys (i.e. same encryption keys))

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Storck to utilize smart card access and processing technologies requiring dual smart cards as taught by Kawan. One of ordinary skill in the art would be motivated to employ Kawan in order to offer enhanced convenience and secure completing transaction utilizing smart card technology. (see Kawan col. 2, lines 12-17)

4. **Claims 18, 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Storck et al.** (US Patent No. 5,434,395) in view of **Findley, Jr et al.** (US Patent No. 5,979,773) and further in view of **Kawan et al.** (US Patent No. 6,289,324).

Regarding Claim 18, Storck discloses a method of securing access to data stored in a personal data storage device comprised of the steps of:

a) storing personal data in a smart card and an enabling key device that are capable of being operably coupled to each other; (see Storck col. 19, lines 51-56: smart card data storage)

c) prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together (see Storck col. 12, lines 45-48: authorization required before transactions, split authorization required two devices coupled together), and Findley discloses wherein prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together (see Findley col. 3, lines 46-51; col. 6, lines 31-33; col. 7, lines 59-65: dual card access system, both cards must be coupled together to be accessible).

b) Storck discloses the usage of encryption technology. (see Storck col. 2, lines 58; col. 19, lines 56-59) Storck does not specifically disclose the usage of encryption keys in the secure protection of data. However, Kawan discloses the usage of encryption keys for encrypting said personal data in the smart card using a first

encryption key and encrypting said personal data in the enabling key device using a second encryption key; (see Kawan col. 5, lines 52-56; col. 9, lines 2-26; col. 10, lines 7-17: encryption key utilization for secure protection of smart card data)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Storck to securely protect data utilizing encryption keys as taught by Kawan, and to utilize smart card access and processing technologies requiring dual smart cards that are operatively coupled as taught by Findley. One of ordinary skill in the art would be motivated to employ Kawan in order to offer enhanced convenience and security completing transactions utilizing smart card technology (see Kawan col. 2, lines 12-17), and to employ Findley in order to enable enhanced and automated user access security features within a network environment (see Findley col. 2, lines 30-32).

Regarding Claim 19, Storck discloses the method of claim 18, wherein said step of prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together (see Storck col. 5, lines 1-7; col. 12, lines 45-48: split authorization requires coupled devices) is comprised of the step of prohibiting the transaction unless the smart card and the enabling key device are coupled together through at least one of wither a wireless data link or a mechanical connector (see Storck col. 8, lines 18-21; col. 10, lines 11-13: connection required for data transactions), and Findley discloses wherein prohibiting the transaction

unless the smart card and the enabling key device are coupled together through at least one of wither a wireless data link or a mechanical connector (see Findley col. 3, lines 46-51; col. 6, lines 31-33; col. 7, lines 59-65: dual card access system, both cards must be coupled together to be accessible).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Storck to utilize smart card access and processing technologies requiring dual smart cards that are operatively coupled as taught by Findley. One of ordinary skill in the art would be motivated to employ Findley in order to enable enhanced and automated user access security features within a network environment. (see Findley col. 2, lines 30-32)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 7:30 am - 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

***

KHS
May 22, 2006

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100